1922

REPORT OF INTERROGATION OF

LTN. ALEX DETTMANN and OBERWACHTMEISTER SERGIUS

SAMSONOW of OKH (Gen. d. NA) at Oberursel, Germany

during August 1945.

This report supplements and expands the long written report prepared by these PWs which is now in Ticom's possession as document T 305.

The present report also contains answers to questions forwarded by Ticom on subjects not covered in the long report, including the locations of fixed W/T intercept stations.

The interrogations were carried out by Capt. James K. Lively assisted by Major W. P. Bundy.

(1) Russian Baudot Traffic

Subjects stated that this was handled by Gruppe VI of
the Gen. d.NA organization, headed by Hptm.ROEDER. The
Section operated first at LOETZEN, later at ZOSSEN, and
finally at ROSENHEIM. Nothing was known of the eventual fate
of the unit. The expert on intercept operation was Wachtmeister
HORCH.

The traffic was largely 5-Z code, mostly NKWD with a
little Army. There was some NKWD 5-Z railway traffic, a
little 4-Z, and some 4 and 5 letter traffic. In 1943-44
there was heavy 3-Z simple code traffic passed by the
"Aeroflot" (civil aviation).

Subjects' own section had examined the 5-Z traffic in
the routine way and in 1944 had spotted six cases of
re-encodement from radio to Baudot (Army, not NKWD). No
messages were solved in these cases.

The "Aeroflot" traffic" was solved by the section,
and very interesting information on fuel supplies and
organization was thought to have been obtained from it.
The traffic averaged 25-30 messages daily. The system was
unenciphered code, with a group representing a full value or
an initial letter only.

In 1944 two men of the section, STEIN and POPPE, had
examined the traffic and done a traffic analysis report on
it. No details of report were known.

The letter traffic had never been solved by Dettman's
section. In 1942-43 they had received much of it, especially
at the time of STALINGRAD, and had given it to OKW/Chi. They
had heard later that no positive results were achieved.
In 1944 Gruppe IV (Wachmeister DOBRING) had solved two
messages in depth. DETTMANN asserts the prevailing belief
that it was machine traffic, and is positive that the
machine was never reconstructed. Almost all 4 and 5 letter
traffic was exclusively Baudot although there was some
4 and 5 letter traffic employed by the Army as practice
traffic. [Subjects stated that the Signaltafeln of Armoured
Units (motorised formations) were sometimes 4 or 5 letter
instead of figure. See diagram on p.35 or report. Subjects
do not know whether RLM/FA worked on machine and/or Baudot
traffic. OKH/Chi had no connection with the Forschungsamt after
1944 when the former organization linked up with OKW/Chi.
However, as a matter of opinion, they do not believe that
FA did.

(2) Machine Systems (see Page 26 of Report)

No machine traffic was passed by Army or Air Force, to
subjects' knowledge nor were machines used by NKWD for purely
military traffic or in the vicinity of the front. Behind the
lines NKWD was believed to employ machines for messages of
political ("defensiv politisch" but not "offensiv politisch"),
economic, or personal content.

Practice traffic was almost invariably manual.

Neither DETTMANN nor SAMSONOW knew what sort of machine the
Russians used but guessed it might be a letter-substitution
similar to the French.

They confirmed the BUGGISCH account of the Russian "K37" in
all particular (See I/ 58 and 64). The machine was captured
and an easy solution method developed by HILBURG and von
DENFFER, but it was not thereafter used.

(3)   CYB (SUW) PROCEDURES (See Page 27 of Report)

        The term "CYB" comprehends all varied camouflaged
communications procedures - not necessarily cryptographic systems -
devised independently after 1942 by Signals Officers for use
on the front. It was not assumed by the Russians that
CYB-procedures would give 100 per cent security. They
remained valid for indefinite periods depending on the
judgment of the Signals Officer who issued them or on suspicion
of compromise. In general, the CYB-systems of the air force remained
in use longer than those of the Army since the former were
amployed behind the lines and were less exposed to capture.
For the various types of systems common under this procedure
see basic chart of Russian systems at end of second Section
of Report.

(4)   BAK-38 (Russian Air Force Code, 1938)

        A page from the BAK-38 code book is represented in
diagram 5 following page 37 of the Report. The page is
divided into ten sections, numbered from 0 to 9, each
section containing ten values. The page number is designated on
a strip down the centre of the page. This strip may be changed
daily. Here the page number may be chosen from three possibilities:
Black 05, Red 67, and Green 59. Each possibility yields
one encipherment.

        If, for example, one wants to read out the letter "C", the
resultant may be: 0565, 6762, or 5965. Element ab is the page
number. Element c is the section number, which, it will be
noted, remains constant. (D. commented that in many Army systems
known to him the last digit remained constant, in which case the
third digit changed.) Element d which represents the code value,
is taken in the case of black encipherment from the first column,
in the case of red from the second column, and in the case of
green from the third column.

        In the written report subjects state that code book contained
approximately 800 values which would indicate a total of 8 pages.
In interrogation the number of pages was said to be 10.

(5)   Use of Tables with Code OKK5

        Explanation of Figure 6 (following p.38). Two tables were
used, each 25 pairs vertically and 20 horizontally. These tables
were double size vertically to enable settings to be made. The
settings were done

                                        /1)

1) vertically, by setting the proper number at the top of the
   page (07 in the right hand table, number folder under and
   out of sight on the left hand table)
2) horizontally, by setting the proper number (14 on the left,
   37 on the right) next to the code book. (There was one
two-digit number every two spaces, reading L. to R., of the
table written at the line. Thus ten setting possibilities
horizontally). The code book was thumb indexed like a
dictionary (represented by the A, S&G, S column) and the
first code pair thus gave the page, being always from the
right hand table.

The page shown in the figure is the "E" page, hence
the first two digits of any value on the page would be 71 or 84.
The last two digits were by column on the page, with the tables
set. Thus, 4017 would be --16; EC --65, X E --86.

(6) "NIWA Code"

This code consisted of 21 pages, each with 100 values. It
was used in the same areas as "ZERNO" and "VIZA". The
reciphering procedure was the same as for "ZERNO".

NIWA, together with ZERNO and VIZA, carried most of the
readable NKWD traffic.

(7) NKWD Railway Code.

This code consisted of 25 pages, each with 100 value.
Each page was divided into four sectors labelled respectively
red, green, yellow, blue. To each coloured quadrant was assigned
a set of numbers, e.g.
        Red - 2,9
        Green - 1,7,8
        Yellow - 3,5
        Blue - 0,4,6
        A code value was then read out as follows:
        ab   equals page number
        c   "   colour
        de   equals location of value on page.

Reciphering of ab and of de was by bigram digit tables,
and of c by single digit tables. For the enciphering of de
there were 4 Tafeln. For the enciphering of ab there were
considerably more than 4 Tafeln.

The solution of the Railway Code was complicated by the
fact that the Russians used no Kenngruppe. However, the code
was broken and 20 to 30 messages per day were read.

(EISENBAHNCODE)

It will be noted that element c serves no purpose whatsoever
other than that of completing the group.

RED		YELLOW	
00		50	
12 APN --------	--------	--------	----- -01 $\frac{2}{9}$ 12
			ab c de
24		74	
GREEN		BLUE	
25		75	
49		99	

Red   2,9
Green   1,7,8
Yellow   3,5
Blue   0,4,6

(8)   Transposition (Wuerfel) Systems (see Page 46 of Report)

Subjects stated that to their knowledge transposition was used only by NKWD in connection with a 4-figure non-alphabetic code. The transposition procedure was a simple one.

The Army and Air Force did not use transposition except for practice traffic.

In guerilla traffic Wuerfel, doppelwuerfel and Raster (including Drehraster) were used but this was very insignificant.

Thus in OKH/Chi there was infrequent occasion to study Wuerfel procedures. (Incidentally,DETTMANN states that during this war the French to his knowledge used the same Wuerfelverfahren as in the first world war. The Germans were thus able to read this traffic. Also the Poles used a simple Wuerfelverfahren and Raster which the Germans were able to read currently before the war.

(9)   Gamma Tables (See Page 47 of Report).

The Gamma Tabellen were so named because the Russians employed the term. There were two kinds of Gamma-Tables,
1) the General Table, used only by the Army, and
2) the Individual Table, used by Army, Air Force and NKWD.

    (1)   General Table (See sketch at end).
          There was no double encipherment in the case
          of the allgemeine Tafel.
          An additive pad (Blocknot) in the General Table
          series consisted of 31 sheets

/(one

(one for each day in the month), divided
into 10 columns and 30 rows. Three digit
indicators stood opposite in the rows and two digit
indicators over the columns. A five-digit
indicator (enciphered) would show where the
encipherer had begun to use the additive: abc being
the row, and de the column. The encipherer would
use the additive to the end of the page and then
return to the top, repeating the process.
Theoretically a page of additive might be used p
to thirteen times.
Subjects stated many of these tables were almost
completely recovered during 1941-42, but
thereafter little success was achieved.

(2) Individual Table
   This additive pad (Blocknot) consisted of 50
   sheets, each sheet to be used only once. Army
   and Air Force pads were drawn up 5 x 10, 6 x 10,
   10 x 10. NKWD pads were 8 x 10 and 20 x 10.
   No indicator was used with the individuelle Tafel
   since the encipherer always started as the upper
   left. If more additive was required after
   finishing a page, the encipherer would use the
   next sheet in the Blocknot.
   A double additive process (Doppelueberwuermung)
   occurred only in the case of NKWD. Here Gamma
   tables were employed in conjunction with a known
   code book, and apparently there were no
   restrictions on the number of times additive could
   be used. In practice NKWD enciphers tended to
   use the same two pages of additive with the result
   that depth could be built up as if only one page
   had been employed.

   GAMMA TABLE (General)

	18	33	41	59	24	07	··	··	··	··
011	11352	78961	32940	38618	·····	·····	·····	·····	·····	·····
034										
172										
112	·····	·····	34281							
148										
179										

   If additive process started with the third square in the
fourth row, the indicator would be 11241. This indicator was in
turn reciphered.

(10) Agent Traffic

The solution of agent, guerilla and "Kundschafter"
traffic was the responsibility of Referat 3c. ("Kundschafter" is
to be distinguished from agent in that the former was more
limited in his mission than the latter. E.g., a Kundschafter
might be sent out to discover amount of traffic passing over
a bridge at a certain time. Also a Kundschafter was more
"localized" whereas the Agent was mobile) Solution depended
mainly on captured material, and there was generally enough
captured material to accomplish solution, Some agent traffic
was one-time tape and therefore unbreakable. By and large the
Gruppe did not place much value on agent traffic and neglected
it.

Subjects were asked of they knew VAUCK. They stated V.
had at one time been with Gruppe IV but had gone to OKW/Chi/WNV
Fu (expansion of WNV Fu unknown to subjects). OKW/Chi they
said handled all agent traffic, whereas Gruppe IV concerned
itself only with military agents.

(11)   Map Coordinate Encipherment

The Kartenplanschette shown on page 50 was used till the
end of 1941. To obtain the cipher reference for a crossroad or
installation, the aperture at the bottom of the planschette
was placed over the name of a known (usually large) locality.
Elements ab of the cipher reference would be the two digits
identifying the known locality. Elements cd would be taken from
the left hand side of the planschette, and elements e from the
top.

From 1942 on a new system was employed, making use of
Gitterkarten. The grid was composed of two-digit numbers at
the left and at the top of the map. Thus a four digit
reference for the place was obtained. To encipher this reference
use was made of two two-digit numbers (these two numbers changing
daily), which were added symbolically to elements ab and cd.

In the case of the planschette 6 digit references might
occur; in the case of the Gitterkarten 5 digit references might
occur. In both instances the additional number was derived from
a further breakdown within the square on the map (giving
locations within 1/9 sq.km.) as below:

1	6	7
2	5	8
3	4	9

The fifth figure in a Gitterkarte reference was
commonly left unenciphered,
Grids on Gitterkarten were changed daily, weekly or
monthly (no fixed period).

Only the Army and Air Force made use of the systems above described.

NKWD always used clear coordinates and depended on the reciphering of the text to disguise geographical references.

Subjects state that coordinate-systems were easy to solve, given sufficient material.

(12) Movement of Eastern Front Field Units.

Subjects listed following locations for signals outfits on the eastern front from beginning of war till its end.

KONA 1:   Vicinity LEMBERG, WINNIZA, POLTAVA, REICHSHOF, CZECHOSLOVAKIAN area.
KONA 2:   WARSAW, BORISOV, ORSCHA, VITEBSK, SMOLENSK, ORSCHA, MINSK, GRODNO, then ORTELSBURG (PRUSSIA), DANZIG, HOLSTEIN area (WISMAR ?).
KONA 3:- RIGA/DUENEBURG, PSKOV, KURLAND (Caught in pocket).
KONA 6:   ROSTOV am DON, NOVOCHERKASSY, MINSK (there newly organized for Partisanenverkehr), Disbanded '44 and assigned to ZOSSEN to OKH/Chi.
KONA 8:   ODESSA, then RUMANIA, KROATIEN, finally LINZ.
FINLAND: Always in area of SALA till disbanded.

(13) Types of 5-digit Traffic ("5Z").

In addition to the main 5Z enciphered code systems, 5Z traffic included the following:

(a) NKWD Railway traffic (See Paragraph 7).
(b) NKWD 3Z code traffic with two dummies added at different points in the groups. Subjects said it was easy to spot the dummies by repeats and consecutive number sequences used.
(c) Special purpose NKWD traffic. This was most often bigram plus trigram substitution by tables 10 x 20 or 10 x 10. The systems were primitive and home made for internal convoy use, for traffic to bands of partisans, and for other prearranged occasions. The keys remained in force only a few days.
(d) Practice traffic, puri qwatsch. This might be random numbers, in which case sequences gave it away, or groups drawn from fixed practice books, read in any order from a page.
     The sum total of all these types of traffic was small compared to that in the main system.

(14) Indicators in the Main 5-digit System.

(a) Individual BLOCKNOTS: there were two indicator froups, the Hinweisgruppe giving the Blocknot number and the Kenngruppe giving the page. The actual Blocknot number had six digits, the first being omitted. The Kenngruppe had two dummy digits, a third digit to indicate whether the Blocknot was General or Individual (neither subjects nor interrogator could see that there was much chance of a coincidence in Blocknot numbers such as to cause confusion.

A set of three digits was allotted to indicate Individual,
another three for General) and two digits to indicate the
page of the Blocknot. The positions of the Hinweisgruppe
and Kenngruppe were constant over periods up to three months,
and could be spotted easily, the Kenngruppe either by common
3rd digits or by the fact that the page number could not go
over 50 (or 31 for General Tables).

> (b) General Blocknots: the system was the
>   same with the addition of a third indicator
>   group. This was itself enciphered by the
>   same page as the message, at the group
>   indicated arbitrarily by the last two digits
>   of the fifteenth (all indicator groups included)
>   group of the text. Thus, if the third
>   indicator group had its position in the first
>   15 groups, it would be left blank until the text
>   had been written out. It would then be
>   enciphered and the resultant group inserted
>   at the proper place. The deciphered group had
>   3 digits for the row indicator and 2 for the
>   column.

(15) SIBERIAN Traffic.

This subject turned out to be a fertile field. The
traffic was almost entirely NKWD, with no Army traffic of
any consequence.

The NKWD organization in SIBERIA was the same as in
the TRANS-CAUCASUS (and in the WHITE SEA area). The top unit
was the Abteilung, with Kommandanturen, and then various types
of small units, as Feldwachen, Kuestenwachen, Posten, and
Manngruppen. The two main areas were the AMUR area and
KASAKSTAN.

The same basic code was used in all areas next to
neutral borders, from IRAN clear to SIBERIA. The Russian
Referat handled all this traffic on a second priority basis,
solving about 40-50% of the neutral area material and
reading about 50 - 60 messages daily. The codes were used
with separate tables for each area, but these were passed
from one area to another and the Siberian area would be
found to use the TRANS-CAUCASUS tables of three months
before. From a crypt standpoint the problems were identical
with other NKWD solutions, and subjects said that they could
have solved even more with additional personnel. The
intercept had no binding priority and was handled by spare
sets, at KOENIGSBERG for SIBERIA and at BRESLAU for the
TRANS-CAUCASUS.

The Siberian NKWD apparently controlled a large amount
of river traffic and was equipped with speed and cannon boats.
It even had a small Air Force of its own, and this had a
separate code up to the beginning of 1942.

(16) Liaison with Japan

The Russian Referat had been visited at LOETZEN in
1942 by two Japanese Officers. D. said they were given a
polite reception but shown very little of anything and no solution work.
They only spent 3-4 hours. The Japs said they had solved the
Russian OKK6 and OKK7, otherwise no 5Z traffic.

(17)   Liaison with FINLAND

        Like other Germans, D. had a high opinion of Finnish
crypt work. He himself had visited FINLAND) in 1942 and
had exchanged technical letters since that time. The first
German Liaison Officer was Hptm. MARQUARDT (later head of
Gruppe I, GEN der NA. Not a crypt man) and he was succeeded
by Oblt. RIEMERSCHMIDT

                                        The Finns had a
liaison officer at LOETZEN from 1942, Oblt. MJE-KOJA (also
not himself a crypt man) and later Oblt. OHN.

        The head of the Finnish crypt section at SORTAVALA
was Hptm. der Reserve Erkki PALE. He had been an
acturical mathematician and became an outstanding cryptanalyst.

        The section had about 60 crypt men. About 20 were in
the front rank, and the stooges were of exceptionally high
quality (according to D., with his own Referat in mind).

        Finnish traffic analysis was as weak as its cryptanalysis
was good, especially by comparison with the work of ZIPPER on
the German side. Contact evaluation was also weak.

(18)   D. threw in some interesting comments at this point on
Evaluation work in General. He believes that this should be
done in the language of the traffic at least in the case of
Russian. The section should be headed by a General Staff
Officer with emphasis on intelligence rather than Signals
training. The OKH Russian evaluation was defective on both
counts. GORZOLLA was not a General Staff Officer and did
not even speak Russian. In 1940 the idea of using Russian
was suggested, but it was dropped to D's regret. The best
man in OKH evaluation was Kriegsverwalfungsrat VOLLMER.

(19)   OBdL Russian Referat. (Chi OBdL Ost II)

        The main Luftwaffe unit was located successively at
MARSTALL, WARSAW, GOLDAP, ZHITOMIR, WARSAW, KOTTBUS and in
the DRESDEN area.

        The chief cryp man was Ltn. von LINGEN, who had
almost 80 people including helpers. Much of there work was
with CYB traffic, which was more abundant than with the Red
Army. It was also less difficult, as it was changed less
often on the more static Air Force nets, and a high percentage
of this was broken.

        The head of Air evaluation was Major KUPFER, with Ltn.
WISSNIKOW. The section had about 30 people and worked in the
Russian language. KUPFER was intelligence liaison officer with
the Luftwaffe Fuehrungsstab.

        There was not a close working relationship between
OKH and the Luftwaffe on Russian crypt.

(20)   Russian Callsigns.

        This was not subject's primary interest, and they did
not do any work on solving the systems. The main enciphered
system was by PT - type tables. The calls themselves were very
varied, common types being ZZ,ZBB,BBZZZ,BBB,BBBB (B = letter,
Z = number).

In general subjects believed that callsigns were
like CYB crypt systems, an individual matter. They did
not believe there was any basic list of calls.

On the whole subject ZIPPER was cited repeatedly.
Subjects said that he was able to maintain continuity on
Russian nets at all times by callsigns and on occasion by
fine differences in radio procedure.

APPENDIX A.

List of Members of the Russian Referat named by
DERRMANN and SAMSONOW. The asterisks indicate the outstanding
men with specialties indicated.

*ANDREJEWSKI, (NKWD)	Harald,	Wachtmeister
BOCK,		Unteroffizier
ESCHLER,	Elmar,	Feldwebel (L)
FEUSTER	Gerhard,	Obergefreiter
FRIEDRICH,	Ernst,	Feldwebel (L)
FRÖMKE,	Igor,	Unteroffizier
GAMAREA,	Nikolaus,	Unteroffizier
* GRACHER, (Air Force)		Obergefreiter
* GRAUDING, (NKWD)	Paul,	Unteroffizier
GROSSE,	Alexander,	Wachtmeister
HELFGEN,	Werner,	Unteroffizier
HENFTLING,		Unteroffizier
HENNINGSON,	Peter,	Obergefreiter
HILLBURG,	Fritz,	Wachtmeister
KONRAD,	Fritz,	Unteroffizier
* KOSTIZIN, (NKWD)	Waldemar,	Obergefreiter
KRIEGEL,	Richard,	Obergefreiter
LANGE,	Erich,	Unteroffizier
LEIBBRANDT,	Gustav,	Wachtmeister
Von LINGEN,	Egon,	Obergefreiter
(not the OBdL man)		
* LOHHOFER,		Wachtmeister
(Agents Esp., also Gen'l		
LUDWIG,	Karl,	Unteroffizier
* MANNEWITZ (NKWD)	Bruno,	Unteroffizier
MUNDT,	Erich,	Obergefreiter
NEUGEBAUER,		Obergefreiter
NITZKI,	Viktor,	Oberwachtmeister
PALKOVITZ,	Franz,	Feldwebel (L)
PANZER,	Kurt,	Unteroffizier
* PAPENDICK,(NKWD)	Georg,	Unteroffizier
POPPE,	Wilhelm,	Wachtmeister
REIMANN,	Karl,	Oberwachtmeister
* Von SELLA, (General)	Roman,	Obergefreiter
* Frh. Von TAUBE, (General)	Georg,	Obergefreiter
SELLNIK,	Hans,	Wachtmeister
* STEIN (Traffic Analysis)	Werner,	Obergefreiter
STEINEMANN,		Wachtmeister
STELTER,	Edmund,	Wachtmeister
STRECKER,	Adolf,	Civilian
THIEL,	Alexander,	Civilian
THOMAS,		Obergefreiter
*Von TOLKACZ, (General)	Martin,	Unteroffizier
Dr. WILLNER,	Franz	Wachtmeister
* ZIPPER (Intercept	Kurt	Oberinspektor
Traffic Analysis)		

DETTMANN - SAMSONOFF

PWs only could give the location of three fixed receiving stations (FESTE HORCHSTELLEN [OST]) and its substations on the German Eastern Front. The sub-stations were mostly located close to the Polish border and served as a sort of cover-up station for tho main receiving (radio) station.

PWs had only a vague, or practically no knowledge at all about the sets and number used, since they were mainly concerned with the handling of incoming messages (translations from Russian into German), rather than with the technical end of it. However, they claimed that BERTA 2 and BERTA 3 - later on also CAESAR-sets were specifically used.

The following fixed receiving stations (FESTE HORCHSTELLEN [OST]) were in operation up to 1939 at:

F.H.ST. KOENIGSBERG

      FESTE WETTER - FUNK - EMPFANGSSTELLEN
      Fixed Weather - Radio - Receiving Stations

Sub-stations $\begin{cases} \text{LYCK} \\ \text{JOHANNISBURG} \end{cases}$

F.H.ST. TREUEN BRIETZEN

        MESERIK
        FRAUSTADT
        SCHNEIDEMUEHL
        SCHLOCHAU

F.H.ST. BRESLAU

        GLOGAU
        LISSA

During the war the main receiving stations (F.H.ST.) were redesignated HAUPTKOMMANDANTUR 3, 2 and 1 respectively, and HAUPT-KOMMANDANTUR // 3 was temporarily in PLESKAU; // 2 in WARSAW, SMOLENSK and MINSK; and // 1 in LEMBERG, and CHARKOW.

Main Receiving Stations F.H.ST. were in command of a

      HAUPTMANN or OBERSTLEUTNANT

Fixed weather - Radio - Receiving Stations (F.W.-F.-E.) were in charge of officials (INSPEKTOREN or OBERINSPEKTOREN.)